



**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

ASST. AUDITOR-CONTROLLERS

ROBERT A. DAVIS
JOHN NAIMO
JAMES L. SCHNEIDERMAN
JUDI E. THOMAS

April 13, 2012

TO: Supervisor Zev Yaroslavsky, Chairman
Supervisor Gloria Molina
Supervisor Mark Ridley-Thomas
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: Wendy L. Watanabe
Auditor-Controller

A handwritten signature in blue ink, reading "Wendy L. Watanabe", is written over the printed name and title.

SUBJECT: **REVIEW OF THE OFFICE OF THE ASSESSOR'S COMPLIANCE WITH
BOARD INFORMATION TECHNOLOGY AND SECURITY POLICIES**

The Board of Supervisors' Information Technology (IT) and Security Policies (Policies) require all departments to comply with the County's IT security standards. The Policies help ensure proper controls and security over the County's IT resources. As required by Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Office of the Assessor's (Assessor or Department) compliance with the Policies, and related County standards and requirements. Our review included testing physical security, antivirus and encryption software, remote access, and IT security awareness training. In addition, because of issues noted during our review, we reviewed the Assessor's IT equipment purchasing, inventory, and disposal/salvage practices.

Results of Review

The Assessor participates in the County's Information Security Steering Committee to stay informed on the latest County IT security requirements and issues. However, the Assessor needs to improve its controls over its IT equipment and practices. Specifically:

- Assessor needs to ensure the Department only purchases IT equipment when it is needed. At the time of our review, the Department had approximately \$654,000 in IT equipment, purchased in Fiscal Years (FY) 2001-02 through 2009-10, that had never been used. This included equipment purchased to use unspent IT procurement funds at the end of some fiscal years, and equipment purchased even though the Department had similar unused items on hand. While it appears the Assessor eventually used some of the equipment, the Assessor may have saved as much as 42% of the cost of the equipment if the equipment was purchased when it was needed.

The Assessor's response (attached) indicates that they have implemented a process to ensure equipment is only purchased when it is needed, and to ensure that they do not have the equipment to be purchased in their existing equipment inventory.

- Assessor needs to evaluate whether staff need more than one computer (e.g., a laptop and a desktop) assigned to them. 342 (24%) of the Assessor's 1,425 employees have two or more computers assigned to them. Some of the staff, who have laptop computers as well as desktops, indicated that they only use the laptops occasionally, and keep them at home when they are not in use. Assigning multiple computers to staff increases the risk of loss, and results in higher maintenance, support, and software costs.

The Assessor's response indicates that they will evaluate whether staff need multiple computers to perform their jobs.

- Assessor needs to improve controls to better safeguard IT equipment. Specifically, the Assessor has not segregated the duties of recording, storing, and issuing IT equipment. In addition, any user of the Assessor's inventory system can delete IT equipment from the inventory system without an independent review/approval. The Department also does not always adequately secure server racks, or lock desktop computers and storage room doors.

The Assessor's response indicates that they have segregated the recording, storing, and issuing of IT equipment, and now require approvals for inventory changes. They also indicated they have secured server racks to the floor, and instructed staff to secure computers and storage rooms.

- Assessor needs to improve its controls over the disposal of surplus IT equipment. The Assessor has not segregated the duties of recommending and authorizing disposal of surplus equipment. In addition, their disposal records were not approved by management, and significantly understated the amount of equipment on hand. For example, Assessor records indicated they had 174 surplus computers, but we counted over 320 surplus computers. We also noted several palettes of used monitors, printers, and other IT devices not included in their disposal records.

It should be noted that Assessor staff initially indicated they did not have any surplus IT equipment. However, we later found that the Department did have surplus equipment in a storage building. When we asked to see the equipment, Assessor staff delayed our access to the storage building. Assessor staff subsequently told us that they had previously moved the surplus items from other locations to the storage building in an attempt to hide the equipment from us.

When we were given access to the building and the surplus IT equipment, we noted that Assessor also stored real property records in the building. County equipment and records should be stored in secured locations. However, the storage building used by the Assessor for the surplus IT equipment and property records was not secured. The building owner had access to the Assessor's storage space, and kept his own car, furniture, and refrigerators in the County-leased space. In addition, the backdoor to the building was unlocked and accessible to the public. The lack of security could result in the loss of County equipment and records.

The Assessor's response indicates they have segregated the duties of recommending and authorizing the disposal of IT equipment. They also indicated an IT manager will ensure disposal records are accurate before obtaining final approvals from their Surplus Property Coordinator and Division Chief of Management Services, and that they have instructed staff to lock the storage building. The Assessor also indicated that they are addressing the issue of hiding equipment with the staff involved.

- Assessor needs to ensure computer data/software is erased (sanitized) before the equipment is salvaged. The Assessor disposed of some equipment, including the surplus equipment discussed earlier, without sanitizing it. Although the non-County agency that received the equipment claimed they had sanitized it, the Assessor does not have documentation to confirm the equipment was sanitized.

The Assessor's response indicates they will work with the agency to establish an agreement for non-disclosure of County information, use of an approved sanitizing method, and that the Assessor will receive documentation of the sanitizing.

- Assessor needs to ensure that all computers have current, functioning antivirus protection. 490 (22%) of the Assessor's 2,192 computers did not have current antivirus protection. Assessor IT staff also did not correct 13 instances where software issues prevented antivirus software from operating properly.

The Assessor's response indicates they will establish procedures to ensure laptops, including those assigned to field staff, are automatically updated as part of their centrally managed antivirus update process. The Assessor will also establish guidelines to monitor and resolve issues that prevent antivirus software from operating properly.

- Assessor needs to limit remote access to County systems to employees who need it. Two (40%) of the five Assessor employees reviewed did not use their remote access from June 2009 through June 2010.

The Assessor's response indicates that they have identified and will discontinue the remote access of those individuals who no longer need it.

- Assessor should evaluate automating/scanning the input of forms, and/or allowing the public to submit forms electronically to help increase efficiency and reduce costs. Assessor staff currently manually input over 1.15 million Homeowner Property Tax Exemption Claim forms and Disabled Veterans Property Tax Exemption applications a year, plus other forms/applications submitted by the public each year.

The Assessor's response indicates that automating Assessor forms is not feasible within the Department's current budget. The Department is currently working to fund the replacement of the old IT systems that use these forms, and eventually automate the processes/forms.

Details of these and other findings and recommendations are included in the attached report. While our review did not disclose any instances of fraud, the weaknesses noted in this report are serious and, if not corrected, could allow losses to go undetected.

Acknowledgment

We discussed our report with Assessor management. The Department's response (attached) indicates general agreement with our findings and recommendations, and that the Department has already implemented some of the recommendations.

We thank Assessor management and staff for their cooperation and assistance during our review. Please call me if you have any questions, or your staff may contact Robert Campbell at (213) 253-0101.

WLW:JLS:RGC:MP

Attachments

c: John R. Noguez, Assessor
Tom Tindall, Director, Internal Services Department
William T Fujioka, Chief Executive Officer
Robert Pittman, Chief Information Security Officer, Chief Information Office
Public Information Office
Audit Committee

REVIEW OF ASSESSOR'S COMPLIANCE WITH INFORMATION TECHNOLOGY AND SECURITY POLICIES

Background

The Board of Supervisors' Information Technology (IT) and Security Policies (Policies) 6.100 to 6.112 require all departments to comply with County IT security standards. The Policies help ensure proper controls and security over the County's IT resources. As required by Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Office of the Assessor's (Assessor or Department) compliance with the Policies, and related County standards and requirements. Our review included testing physical security, antivirus and encryption software, equipment disposition, remote access, and user security awareness training. Because of issues noted during our review, we expanded our scope to include IT equipment purchasing, inventory, and disposal/salvage.

IT Equipment Inventory

County Fiscal Manual (CFM) Section 4.1.3 requires departments to ensure items purchased are necessary for their work. CFM Section 5.2.6 also requires departments to take action to address obsolete/overstocked items.

We noted the Assessor had approximately \$654,000 in unused IT equipment in inventory, including servers, computers, printers, and flash drives purchased between Fiscal Years (FY) 2001-02 through 2009-10. The equipment included purchases made to use unspent IT procurement funds at end of the fiscal years, items purchased without ensuring staff could use them, and items purchased even though the Department had similar unused items on hand. For example, during FY 2007-08, the Department made multiple purchases of a total of approximately 150 desktop computers, even though they had 28 similar new computers on hand that they could have used. The Department never used the 28 computers they already had on hand, and only used 120 of the 150 additional computers they bought.

Although the Assessor eventually did use some of the \$654,000 in equipment they had in inventory, they might have paid less if they had purchased the equipment when it was needed. For example, we reviewed 278 items, with a total cost of \$221,689, that the Assessor used from the inventory, and noted they could have saved approximately \$93,000 (42%) if they had purchased the items, or the equivalent, when they were actually needed since the cost of IT equipment often decreases over time.

Recommendations**Assessor management:**

1. **Monitor IT equipment purchases, and only purchase equipment when it is needed.**
2. **Evaluate the IT equipment inventory, and transfer or salvage obsolete/overstocked items.**

Staff Computer Assignments

The Assessor's records indicate that 285 (24%) of the Department's 1,425 employees have two computers (e.g., a laptop and a desktop) assigned to them, and another 57 (4%) employees have three or more computers. Some Assessor staff who have two computers indicated that they only use their laptops occasionally, and keep them at home when they are not in use. Assigning multiple computers to staff increases the risk of loss, and results in higher maintenance, support, and software costs.

Assessor management should evaluate whether staff need multiple computers assigned to them, including whether staff who regularly work offsite should have only a laptop, and consider establishing a laptop pool and checkout process.

Recommendation

3. **Assessor management evaluate whether staff need multiple computers assigned to them, including whether staff who work offsite should have only a laptop, and consider establishing a laptop pool and checkout process.**

Physical Security and Equipment Control

Policy 6.106 requires departments to safeguard IT equipment. CFM Section 8.2.4 also requires departments to maintain an up-to-date inventory list of IT equipment and its location to assist in safeguarding assets.

We selected 34 laptop computers from the Department's inventory list, and noted:

- Two (6%) laptops could not be found. One laptop may have been salvaged, but the Department could not provide documentation of this. The other laptop was previously reported as lost, and should have been removed from the Department's inventory list.
- Two (6%) laptops were in employees' cars. Assessor management should remind staff not to store laptops in vehicles as required by the Laptop Handling Guidelines (County IT Policy 6.110, Attachment 110.01).

We also noted the following weaknesses in the Department's controls over its IT equipment:

- The Assessor's non-capital asset list (which includes the IT equipment) contains incomplete/inaccurate data, including missing or incorrect asset custodians, locations, asset tag numbers, serial numbers, and descriptions.
- Any user of the Assessor's IT equipment inventory system can delete items from the system without an independent review or approval. Assessor management should require review/approval for inventory system transactions, or use the eCAPS Inventory Management Module to control non-capital IT equipment.
- Assessor management does not always segregate the duties of recording, storing, and issuing IT equipment. We noted the Information Technology Division (ITD) staff, who are custodians of the equipment, issue equipment to staff and update the inventory system without an independent approval. Assessor management should transfer custody over ITD inventory to the main warehouse, and remove ITD staff's ability to add/remove items from the inventory system.
- Department staff do not always lock/secure their computers, or close the door to the IT equipment storage room. In addition, the Department has some server racks that are not secured to the walls or floors to prevent damage in an earthquake.
- Some IT equipment did not have County tags because the tags had fallen off.
- The Department does not properly conduct annual physical inventories as required by CFM Section 6.8.2. Assessor management indicated they performed a physical inventory three months before our review, but as noted earlier, we noted their inventory list was not accurate.

Assessor management needs to strengthen physical security and controls over equipment by implementing the following recommendations.

Recommendations

Assessor management:

4. **Ensure the non-capital asset inventory list is properly updated, and contains accurate information, such as asset custodians, locations, tag numbers, serial numbers, brands, and models.**
5. **Require at least one level of review/approval for inventory system transactions, or use the eCAPS Inventory Management Module to manage/control non-capital IT equipment.**

6. **Transfer control over ITD inventory to the main warehouse, and remove ITD staff's ability to add/remove items from the inventory system.**
7. **Remind staff to not leave laptops in their cars, and lock/secure computers and storage rooms.**
8. **Bolt unsecured server racks to the wall or floor.**
9. **Ensure County IT equipment is properly tagged.**
10. **Ensure staff properly conduct and document annual physical inventories.**

Disposal Procedures

CFM Section 6.10.2 requires departments to prepare a list of equipment to be disposed of for management's review and approval. The County's Disposal Procedures also require that two individuals be involved in disposing of surplus property. Departments must also offer surplus IT equipment to other County departments first, and then to all County-approved agencies to provide an equal opportunity to all the agencies.

We noted that the Assessor had a significant amount of surplus used IT equipment, and that their disposal records significantly understated the amount of equipment on hand. Specifically, the Department's records indicated they had 174 surplus computers, but we counted over 320 computers. In addition, we noted several palettes of used monitors, printers, and other computer equipment that were not included on their disposal records, and their records were not approved by management.

It should be noted that Assessor staff initially indicated they did not have any surplus IT equipment. However, we later found that the Department did have surplus equipment in a storage building. When we asked to see the equipment, Assessor staff delayed our access to the storage building. Assessor staff subsequently told us that they had previously moved the surplus items from other locations to the storage building in an attempt to hide the equipment from us.

When we were given access to the building and the surplus IT equipment, we noted that Assessor also stored real property records in the building. County equipment and records should be stored in secured locations. However, the storage building used by the Assessor for the surplus IT equipment and property records was not secured. The building owner had access to the Assessor's storage space, and kept his own car, furniture, and refrigerators in the County-leased space. In addition, the backdoor to the building was unlocked and accessible to the public. The lack of security could result in the loss of County equipment and records.

We also noted that the Assessor does not comply with other County requirements for disposing of surplus equipment. Specifically:

- The Assessor does not segregate the duties of recommending and authorizing the disposal of surplus property. We noted that the same individual who identified and recommended the disposal of surplus equipment also authorized the disposal. To reduce the risk of loss, Assessor management should ensure that at least two individuals authorize the disposal of surplus property as required by the County's Disposal Procedures.
- The Assessor did not offer surplus IT equipment to other County departments or to all County-approved agencies as required by the County's Disposal Procedures. Although the Assessor donated the equipment to an approved agency, the Department needs to ensure it offers the equipment to other County departments first, and then to all eligible agencies.

Recommendations

Assessor management:

- 11. Keep an approved and complete record of its surplus equipment, and secure the surplus equipment storage facility.**
- 12. Segregate the duties of recommending and authorizing the disposal of surplus property.**
- 13. Offer surplus IT equipment to other County departments first and then to all County-approved agencies.**

Erasing County Data/Software

Policy 6.112 requires departments to erase all data/software from IT equipment (sanitize) before disposing of it. The Hard Drive Cleaning Standard requires departments who use contractors to sanitize equipment to have a signed agreement covering non-disclosure of County information, use of a County-approved sanitizing method, and documenting the sanitizing of each device.

The Assessor donated its IT equipment to an agency that redistributes it to schools and non-profit organizations. Although the agency indicated they sanitize the equipment, the Assessor does not have an agreement with the agency for the sanitizing service. The Assessor also cannot document that all equipment has been sanitized because staff do not prepare itemized lists of all equipment given to the agency, or get documentation that to confirm the equipment was sanitized.

Recommendations

Assessor management:

14. Establish an agreement with any agency receiving Assessor IT equipment covering sanitizing the equipment, including non-disclosure of information, use of an approved sanitizing method, and documentation of the sanitizing.
15. Maintain an itemized list of all donated IT equipment that must be sanitized, and obtain documentation from the agency that each item has been sanitized.

Antivirus Protection

Policy 6.102 requires departments to ensure they have functioning up-to-date antivirus protection for all County computers.

The Assessor's records indicated that 490 (22%) of the Department's 2,192 computers did not have current and/or operating antivirus protection. We noted the protection was out-of-date and/or not operating because the computers had not been used for an extended period, because known software issues had prevented the antivirus program from operating, or other issues. In addition, we noted that Assessor IT staff did not take any action to resolve 13 instances where software issues prevented antivirus protection from operating properly.

Assessor management should ensure staff update their antivirus protection by regularly connecting their computers to the Department's network, or to the appropriate antivirus website.

Recommendations

Assessor management:

16. Ensure staff update their antivirus protection by regularly connecting their computers to the Department's network, or to the appropriate antivirus website.
17. Ensure IT staff promptly resolve software issues that prevent antivirus protection from operating properly.

Network Scan

Policy 6.101 requires that County IT resources be used only for County business. Policy 6.105 prohibits County IT users from downloading unauthorized software or other inappropriate content. Departments can perform network scans to monitor for compliance with these Policies.

We noted that the Assessor does not perform these scans. While we did not find any unauthorized software or inappropriate content during our review, the Assessor should perform these scans to help monitor for Policy compliance.

We also noted that the Assessor used to scan their network for open network connections and other vulnerabilities, but stopped in 2008, because the County's network intrusion software blocks the scans. However, departments can request the Internal Services Department (ISD) to allow a scan to be done. Assessor management should work with ISD to periodically perform network vulnerability scans.

Recommendations**Assessor management:**

- 18. Periodically scan their network for unauthorized software and inappropriate content.**
- 19. Work with ISD to periodically perform network vulnerability scans.**

Remote Access

Departments can give individuals remote access to County systems by issuing them a "VPN token". Policy 6.101 requires management approval for all remote access. Assessor management did not have approval documentation for any of the ten remote access users we reviewed. Although Assessor managers confirmed all ten user's access was appropriate, management should have documented approvals on file.

We also noted that two (40%) of the five employees reviewed did not use their remote access at all from June 2009 through June 2010. Since there are costs associated with issuing VPN tokens, the Assessor should evaluate whether staff need their remote access.

Recommendations**Assessor management:**

- 20. Ensure documented approvals are on file for all remote access users.**
- 21. Evaluate whether staff need their remote access.**

IT Security Training

Policy 6.111 requires departments to provide IT Security Awareness Training to all County IT users to ensure they are aware of their responsibilities for information security. This training should be conducted during new employee orientation, and periodically thereafter. Departments should document that employees complete the training.

Assessor records show that 186 (13%) of the 1,425 Assessor employees had not completed all the required training. Specifically, 140 users were not trained on Policies 6.109 through 6.112, which were introduced between May and October 2007. Another 46 County employees and two contract (non-County) employees with County-issued computers have not received any IT security training. Assessor management should ensure all IT users receive IT Security Awareness Training, and that the training is properly documented.

Recommendation

- 22. Assessor management ensure all IT resource users receive IT Security Awareness Training, and that the training is documented.**

Electronic Submission of Assessor Forms

We noted that Assessor staff manually input over 1.15 million Homeowner Property Tax Exemption Claim forms and Disabled Veterans Property Tax Exemption applications, plus other forms/applications received from the public each year. To increase efficiency, reduce printing and storage costs, and improve input accuracy, Assessor management should evaluate automating/scanning form input, and/or allowing the public to submit the forms electronically.

Recommendation

- 23. Assessor management evaluate automating/scanning form input, and/or allowing the public to submit the forms electronically.**

Standards and Procedures

CFM Section 8.2.3 requires departments to have standards and procedures to guide supervisors and staff in performing their duties. We noted that the Assessor does not have written standards/procedures for some of the processes we reviewed, including:

- Disposing of surplus IT devices
- Physical security and control over equipment (non-capital assets)
- Evaluating IT equipment acquisition
- Reviewing unused IT equipment inventory
- Updating virus definitions and resolving antivirus software issues

- Performing network scans
- Maintaining remote access authorization forms
- Conducting an IT risk assessment

Recommendation

- 24. Assessor management develop written standards/procedures for the eight areas identified above.**

IT Risk Assessment

Policy 6.107 requires departments to identify their critical IT services, and assess their information security risks as part of the Auditor-Controller's Internal Control Certification Program (ICCP). Departments must certify that proper controls are in place, or that action is being taken to correct any weaknesses or vulnerabilities.

Many of the weaknesses/vulnerabilities noted in our review should have been detected when completing the ICCP. However, the Assessor's most recent certification indicated that the appropriate controls were in place.

To help Assessor managers evaluate and improve internal controls over IT and security, management should ensure staff perform and document information security risk assessments by properly completing the ICCP, and develop corrective action plans to address any identified control weaknesses.

Recommendation

- 25. Assessor management ensure staff perform and document IT risk assessments by properly completing the Internal Control Certification Program, and develop corrective action plans to address any identified control weaknesses.**



**OFFICE OF THE ASSESSOR
COUNTY OF LOS ANGELES**

320 KENNETH HAHN HALL OF ADMINISTRATION
LOS ANGELES, CALIFORNIA 90012-2770


(213) 974-3101

assessor.lacounty.gov

JOHN R. NOGUEZ
ASSESSOR

March 29, 2012

TO: Wendy L. Watanabe
Auditor Controller

FROM: John Noguez 

SUBJECT: **REVIEW OF ASSESSOR'S COMPLIANCE WITH INFORMATION TECHNOLOGY
AND SECURITY POLICIES**

Attached is our response to the audit performed by your department of the Assessor's compliance with IT and security policies.

As indicated in our response, we agree with all the findings and have already began implementing remedies to address those areas where we were not in compliance. We will also assign staff from our Quality and Efficiency Unit to do a follow up review in order to ensure we continue to adhere with established policies and procedures.

I would like to thank you and your staff for bringing to our attention the weaknesses in question. We are bound to have stronger operations as a result of the audit.

Please feel free to call me if you have any questions. Your staff may call Anne Suarez, Administrative Deputy at (213) 974-3182.

JN:RH
c: G. Renkei
A. Suarez

Attachment

Review of Assessor's Compliance with Board IT Policies

Recommendations

Assessor management:

- 1. Monitor IT equipment purchases, and only purchase equipment when it is needed.**

Assessor's Response

We agree. A process was implemented to determine if a piece of equipment is truly needed or if it is available among the surplus items, before a purchase is made.

- 2. Evaluate the IT equipment inventory, and transfer or salvage obsolete/overstocked items.**

Assessor's Response

We agree. The Assessor's Procurement staff have for some years been preparing lists of the equipment that had been housed in the warehouse for a year or longer. Those lists will now include all equipment located in the warehouse regardless of when received. Doing so will give us a better understanding of what's available.

Additionally, we have established a committee consisting of staff from the IT and Management Services Divisions that meet regularly to review those lists and by doing identify those that can be transferred or salvaged.

- 3. Assessor management evaluate whether staff need multiple computers assigned to them, including whether staff who work offsite should have only a laptop, and consider establishing a laptop pool and checkout process.**

Assessor's Response

We agree. We will review the list of users with multiple computers assigned and evaluate the needs to perform their jobs.

4. **Ensure the non-capital asset inventory list is properly updated, and contains accurate information, such as asset custodians, locations, tag numbers, serial numbers, brands, and models.**

Assessor's Response

We agree. Access to the inventory system was previously available to departmental staff not affiliated to staff in the Procurement Unit (warehouse). As such there were instances when the information in the system could be changed without the knowledge of the department's Procurement Supervisor. That will no longer be the case. The ability to make changes to the system will be restricted to the warehouse staff to ensure the accuracy of the information.

5. **Require at least one level of review/approval for inventory system transactions, or use the eCAPS Inventory Management Module to manage/control non-capital IT equipment.**

Assessor's Response

We agree. Currently all changes that need to be made to the system are written on the Assessor's Inventory Record Update form which requires the signature of the Procurement Supervisor before the changes are made.

6. **Transfer control over ITD inventory to the main warehouse, and remove ITD staff's ability to add/remove items from the inventory system.**

Assessor's Response

We agree. Control of this inventory system is now restricted only to staff in the main warehouse and it is accessible by Information Technology Division (ITD) staff as view only. IT staff can no longer access the system to change its contents.

7. **Remind staff to not leave laptops in their cars, and lock/secure computers and storage rooms.**

Assessor's Response

We have issued a memo to all users to secure desktop and laptop computers and to report to the IT Help Desk if their desktops are not secured so that steps to do so are taken.

We have issued "Laptop Handling Guidelines" to all users which include among other instructions that laptops are not to be left unattended or in cars.

8. Bolt unsecured server racks to the wall or floor.

Assessor's Response

All serves have been bolted down to the floor

9. Ensure County IT equipment is properly tagged.

Assessor's Response

We agree. All equipment is tagged when it is first received in the warehouse. Additionally, whenever a physical inventory is performed the practice has been to tag a barcode to those items without a tag. The barcode is then entered into the system. A top-to-bottom physical inventory was performed throughout the department in October 2011. A tag was attached to those items that did not have one.

10. Ensure staff properly conduct and document annual physical inventories.

Assessor's Response

We agree. As the audit report indicates, an annual inventory had been performed three months prior to the Auditor Controller's review. An inventory was again performed in October 2011 by staff that are knowledgeable with the inventory process.

11. Keep an approved and complete record of its surplus equipment, and secure the surplus equipment storage facility.

Assessor's Response

We agree. The Assessor's Procurement staff have for some years been preparing lists of equipment that had been housed in the warehouse for a year or longer. Those lists will now include all equipment located in the warehouse regardless of when received. Doing so will give us a better understanding of what's available. Additionally, staff have been instructed to ensure the surplus equipment storage facility is locked when not in use.

- 12. Segregate the duties of recommending and authorizing the disposal of surplus property.**

Assessor's Response

We agree. Effective immediately at least two individuals will be involved in the disposal of equipment: The Department surplus Property Coordinator (DSPC) and the Division Chief of Management Services will have final approval. A third and fourth person will be involved if the items to be disposed of involve IT equipment. The third person will recommend the disposal and the fourth will be an IT manager who will authorize the disposal before forwarding the list to the DSPC.

- 13. Offer surplus IT equipment to other County departments first and then to all County-approved agencies.**

Assessor's Response

We agree. Items to be donated will be posted on the County's surplus web page to make the equipment available first for County's re-distribution. It is our understanding that if the donated items are not picked up by another County department within 12 days after having been posted, the items will automatically roll over to the County Donation Web page.

- 14. Establish an agreement with any agency receiving Assessor IT equipment covering sanitizing the equipment, including non-disclosure of information, use of an approved sanitizing method, and documentation of the sanitizing.**

Assessor's Response

We agree. There should be documentation that items donated have been sanitized. We have received such documentation in the past from the agency we've used. We will contact the donation agency to discuss establishing an agreement that describes the non-disclosure/confidentiality of County information, use of an approved sanitizing method and documentation of the sanitizing.

- 15. Maintain an itemized list of all donated IT equipment that must be sanitized, and obtain documentation from the agency that each item has been sanitized.**

Assessor's Response

We agree. We will maintain a list of donated equipment that must be sanitized and obtain documentation from the donation agency that each item has been sanitized.

- 16. Ensure staff update their antivirus protection by regularly connecting their computers to the Department's network, or to the appropriate antivirus website.**

Assessor's Response

The Department has for some years established an antivirus system to centrally manage all computers' antivirus software with automatic updates. Inactive devices are updated prior to deploy into production. In addition the Department is establishing a procedure whereby laptops will be automatically updated with the most current antivirus definition. This will also include laptops used by staff involved in field audits.

- 17. Ensure IT staff promptly resolve software issues that prevent antivirus protection from operating properly.**

Assessor's Response

Assessor staff is actively monitoring and resolving antivirus issues using the County standard endpoint protection system. It's not unusual to have unresolved instances of antivirus software at any given time. To improve the process, the Department is establishing guidelines for staff to monitor and resolve endpoint protection software issues that prevent the antivirus protection from operating properly.

- 18. Periodically scan their network for unauthorized software and inappropriate content.**

Assessor's Response

We have sent a reminder to all employees that it is prohibited to store or download non-work related files. The Department is establishing a system to scan for unauthorized software and inappropriate content.

- 19. Work with ISD to periodically perform network vulnerability scans.**

Assessor's Response

The Department is participating in the Countywide Enterprise McAfee Vulnerability Management (MVM) to scan all servers. This system is managed by ISD and scans automatically per County schedule

- 20. Ensure documented approvals are on file for all remote access users.**

Assessor's Response

The Department currently keeps scanned copy of all remote access registration forms on a server to document approvals for all users with remote access. The Department is preparing procedures for maintaining remote access authorization forms.

- 21. Evaluate whether staff need their remote access.**

Assessor's Response

We agree .We have surveyed all employees who have remote access to County IT resources and identified those who have no legitimate business need for it. We are in the process of discontinuing those individuals. We will review the user list annually and will not renew the Secure-Token if it's determined that the user no longer needs it.

- 22. Assessor management ensure all IT resource users receive IT Security Awareness Training, and that the training is documented.**

Assessor's Response

We agree. Training on IT security awareness was provided by the end of the 2011 calendar year to those employees who had not taken it.

- 23. Assessor management evaluate automating/scanning form input, and/or allowing the public to submit the forms electronically.**

Assessor's Response

We agree that many functions and operations in this department as well as in other County departments could benefit from automation. The recommendation that we should evaluate automating data entry of Homeowner Exception claims and Veterans Property Tax applications is a worthwhile suggestion. However, actually pursuing this endeavor would seem to carry a price that is beyond our current available funding. The Assessor is committed to automating functions and processes that increase productivity and efficiency and over the years have implemented several projects with that in mind. Our main goal in this regard is to replace legacy systems some of which date back to the 1960s and eventually automate processes such as the data entry noted in this finding.

- 24. Assessor management develop written standards/procedures for the eight areas identified above.**

Assessor's Response

The department is preparing standards/procedures to address Auditor's recommendations.

- 25. Assessor management ensure staff perform and document IT risk assessments by properly completing the Internal Control Certification Program, and develop corrective action plans to address any identified control weaknesses.**

Assessor's Response

We agree. We have established an Audit Section and will have staff from that section review existing IT practices to ensure controls are in place or to correct weaknesses or vulnerabilities. This will enable us to properly complete the ICCP.